Михайлишина Анастасия Андреевна
бакалавр юрид. наук, студентка
ФГБОУ ВО «Ульяновский государственный
педагогический университет им. И.Н. Ульянова»
г. Ульяновск, Ульяновская область

ПЕРСПЕКТИВЫ ВОВЛЕЧЕНИЯ В УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ДОКАЗЫВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ

Аннотация: *несмотря на распространенность преступлений, совершаемых с помощью технических устройств, в настоящее время недостаточно конкретизирован процессуальный порядок изъятия и фиксации следов, оставляемых в результате киберпреступлений и других преступлений. Рост киберпреступности напрямую связан с доступностью и популярностью цифровых технологий, и для раскрытия данных преступлений, прежде всего, следует использовать новые источники доказательств.*

Ключевые слова*: биометрические данные, киберпреступность, доказательства, современные технологии, идентификация личности.*

Для совершенствования законодательства и в целом перспективы использования технических средств в уголовном судопроизводстве необходимо искать способы наиболее эффективного использования цифровых технологий, а также разрабатывать методики по экспертной оценке данных материалов, оснащать криминалистические лаборатории соответствующей техникой и программным обеспечением [4, с. 161]. Например, для видеофиксации все чаще начинают использоваться биометрические системы контроля, которые в соответствии с международной терминологией характеризуются точностью опознания: FAR (False Acceptance Rate) – ошибка (вероятность) принять «чужого» за «своего» / ошибка пропустить «чужого» или FRR (False Rejection Rate) – ошибка (вероятность) принять «своего» за «чужого» / отказать в доступе «своему» [3, с. 85].

Но внедрение в практическую деятельность данных источников доказательств тормозит несколько факторов. К ним можно отнести нехватку каче-

ственной видеоаппаратуры, квалифицированных специалистов по видеотехнике, низкий уровень подготовки следственных работников, а также недостаточную правовую регламентацию ее использования [3, с. 86].

Начальник ГУЭБиПК МВД России генерал-лейтенант полиции Андрей Курносенко в своём выступлении на пресс-конференции, посвященной вопросам выявления и пресечения преступлений в сфере экономики, совершаемых с использованием IT-технологий, отметил, что существует динамика прироста таких преступлений и за прошедшие 3 года она составила 165%. Сотрудниками органов внутренних дел за 10 месяцев 2019 года задокументировано 236,4 тыс. IT-преступлений. Основной их массив составляют различные виды мошенничеств, на долю которых приходится около половины всех зарегистрированных преступлений. На сегодняшний день каждое седьмое преступление совершается с использованием IT-технологий. Размер причиненного материального ущерба в текущем году превысил десять миллиардов рублей [1].

Рост киберпреступности напрямую связан с доступностью и популярностью цифровых технологий. Тенденция внедрения в жизнь людей электронных технологий вызывает у пользователей определенную зависимость: мы не можем сейчас представить свой день без социальных сетей, различных мессенджеров; создан портал «Госуслуги», представляющий собой совокупность электронных сервисов. Все эти данные могут стать объектом киберпреступления, и доказательства по ним можно получить только с помощью новых современных технологий.

Для раскрытия современных преступлений применяют достаточно новые доказательства, которые уже применяется в других странах, это биометрические данные. Помимо традиционных видов биометрических данных (отпечатки пальцев, сетчатка глаза), к ним также относятся биометрия походки, биометрия нажатия клавиш, биометрия запаха. Например, в Китае уже вводится автоматическая программа идентификации личности по походке. Для работы программы идентификации нужна только камера, находящаяся на расстоянии 50 метров от цели. Данная программа основывается на уникальном рисунке походки, вклю-

чая ритм, скорость и другие особенности передвижения. Как говорит исследователь Института автоматизации при Китайской академии наук (CAS) Хуан Юнчжэнь, новая технология работает в десятки раз быстрее и дальше, чем сканеры радужной оболочки глаза [2].

В Соединенных Штатах Америки (далее США) биометрические данные не только изучаются, но и применяются в качестве доказательств. Новейшей разработкой также считается биометрия походки. Её характеризуют как своеобразный способ ходьбы, представляющий сложную пространственно-временную биометрию. Данный способ идентификации личности может быть произведен из любой отдаленной точки. Поскольку походка является уникальной, прежде всего, она зависит от ряда факторов, например масса тела, поверхность ходьбы, обувь, одежда [6].

Еще одним достаточно новым видом установления личности по биометрическим данным в США является биометрия нажатия клавиш. Считается, что каждый отдельный рисунок слов и предложений набирается на клавиатуре уникальным способом. С помощью этого и устанавливается биометрия, при этом эти данные не являются особо отличительными в плане распознавания человека, но они помогают дать определенную характеристику его личности, например, характер, стиль письма, в каком состоянии человек находился во время набора клавиш. Рисунок нажатия клавиш также зависит от эмоционального состояния, положения и типа клавиатуры. Преимущества использования данной биометрии в том, рисунок нажатия клавиш можно наблюдать незаметно, с помощью специализированных программ. Но поскольку данный способ идентификации личности затрагивает конституционные права, необходимо получить постановление суда об изъятия и копировании информации с электронных носителей информации при производстве следственных действий [6].

Помимо перечисленных выше видов биометрических данных, традиционно еще выделяют:

1) биометрию отпечатков пальца;

2) биометрию лица;

3) биометрию радужки;

4) биометрию ДНК;

5) биометрию голоса.

В США в штате Калифорния биометрия лица впервые стала одним из доказательств по уголовному делу. Камеры наблюдения на доме засняли человека, подозреваемого в совершении убийства и ограбления. Адвокат обвиняемого предоставил неподвижные кадры с видеозаписи вместе с показаниями эксперта по биометрии, который сравнил фотографию подсудимого и данный кадр. Экспертиза показала несовпадение лица, изображенного на фотографии и на неподвижном кадре данной видеозаписи [5]. К сожалению, суд присяжных не принял во внимание эти доказательства и вынес обвинительный вердикт, но дело не стало прецедентным, поскольку рассматривалось не в Верховном суде США. Можно сделать вывод, что такие виды биометрических данных, как биометрия лица и голоса, требует подтверждения эксперта для соблюдения достоверности, допустимости и относимости данных доказательств.

По нашему мнению, технология идентификация личности вполне может стать новым источником доказательств, видом электронных доказательств, т.е. данных, полученных с помощью электронно-вычислительных систем, в данном случае это камеры, компьютеры, программы и т. п. При этом такие виды биометрических данных, как биометрия лица и голоса, требуют подтверждения эксперта.

Таким образом, анализируя статистику, можно сказать, что число пользователей смартфонов, других современных технических средств, сети Интернет увеличивается, поэтому и перспектива вовлечения новых доказательств становится острой проблемой для расследования преступлений. Система биометрических данных во многом упрощает работу правоохранительных органов по получению сведений, имеющих значение для дела. Поэтому мы предлагаем закрепить процесс использования подобной значимой информации в процессе доказывания в качестве подвида новых источников – электронных доказательств, поскольку это будет способствовать сокращению сроков расследова-

ния, упрощению работы следователей, а также раскрытию новых видов преступлений, совершаемых с помощью технических средств.

Список литературы

1. Андрей Курносенко рассказал о выявлении и пресечении киберпреступлений в сфере экономики [Электронный ресурс]. – Режим доступа: https://мвд.рф/news/item/19087056

2. Новая технология слежки установит личность по походке [Электронный ресурс]. – Режим доступа: https://hitech.vesti.ru/article/683834

3. Тульских В.Д. К проблеме использования цифровой аудио- и видеозаписи в уголовном процессе / В.Д. Тульских // Армия и общество. – 2012. – №4 (32). – С. 83–88.

4. Тульских В.Д. Использование биометрических технологий в экспертно-криминалистической деятельности / В.Д. Тульских // Армия и общество. – 2013. – №1 (33). – С. 161–165.

5. A first: biometrics used to sentence criminal [Электронный ресурс]. – Режим доступа: http://www.homelandsecuritynewswire.com/first-biometrics-used-sentence-criminal

6. Monika Saini. Anup Kumar Kapoor. Biometrics in Forensic Identification: Applications and Challenges [Электронный ресурс]. – Режим доступа: https://www.omicsonline.org/open-access/biometrics-in-forensic-identification-applications-and-challenges-2472–1026–1000108.php?aid=76775